Dell KACE K1000 Systems Management Appliance
Version 6.0

Release Notes

About these release notes

These release notes provide information about Dell KACE K1000 appliance (server) and K1000 Agent version 6.0.

Topics include:

- New features and enhancements on page 1
- End-of-life features on page 8
- System requirements on page 9
- Updating the K1000 appliance (server) on page 9
- Upgrading Agent software on managed devices on page 13
- Stopping and starting the Agent on page 15
- Resolved issues on page 15
- Known issues on page 19
- Global support on page 24

New features and enhancements

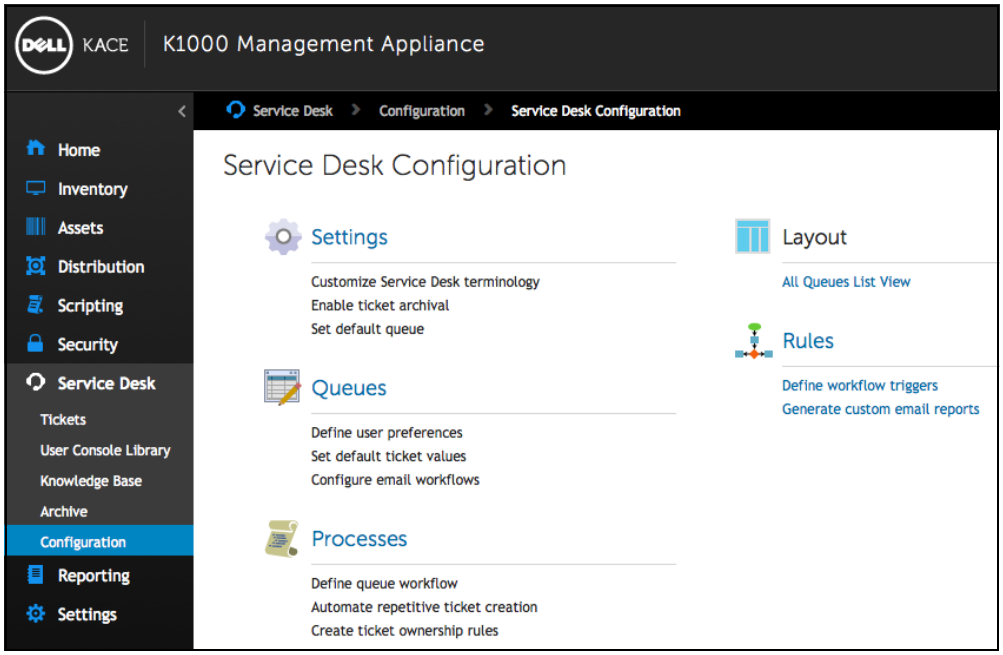
Version 6.0 introduces a new user interface design and features such as Discovery, Agentless device inventory, and Application Control.

New user interface design

The K1000 user interface has been redesigned to improve the user experience. Changes include:

- **Modernized look and feel**: Colors, controls, and other interface elements have been re-designed to improve usability in both the Administrator Console and the User Console.

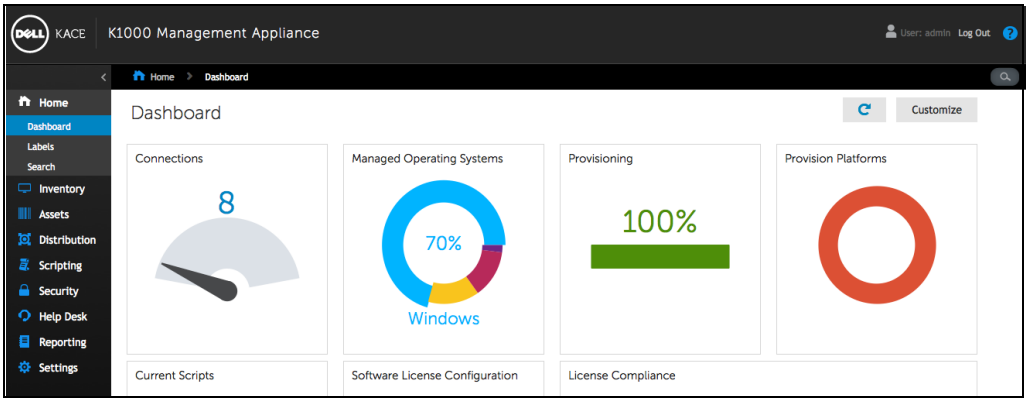
- **Improved navigation**: A left navigation bar has been introduced to save space and improve access to features.
- **Improved panel display**: Options have been moved to panel pages to improve access. Graphs from panel pages have been moved to the new Dashboards.



- **Customizable list pages**: Columns on list pages can be resized, repositioned, and sorted. In addition, you can specify whether to refresh list pages automatically, at a specified interval, or not at all, and you can choose the number of items to display. User preferences persist throughout a login session.
- **Standardized actions and objects**: Actions such as creating Smart Labels have been standardized across components, such as Inventory and Patching.
- **Improved forms**: Forms and configuration pages have been redesigned to eliminate the need for explicit Edit buttons. Field validation, and actions such as Duplicate and Cancel, have also been improved.
- **Improved wizards for labels**: The wizards used to create labels now use metadata and provide search capability.
- **Service Desk improvements**: A rules engine has been introduced to improve the management of Service Desk Ticket Rules.

Dashboards

New Dashboards provide central access to important information through customizable and resizable widgets. If the Organization component is enabled, Dashboards are available at the organization and appliance level.



About data presented in widgets

Most Dashboard widgets display cached data, and the database queries that refresh data run on schedules that are appropriate for the data sources. For most widgets, queries are performed every five minutes or every hour. However, some queries have the potential to run for several minutes, and these queries run less frequently to reduce the processing impact on the appliance. As a result, the following widgets display data that can be up to eight hours old:

- License Compliance
- Disk Capacity
- Patch Installation Progress
- Patching Tasks Completed
- Critical Patch Compliance

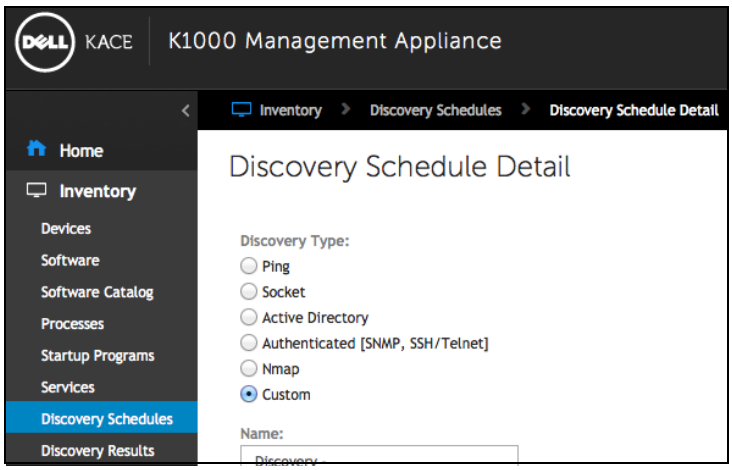
Device Discovery

The IP Scan component has been replaced by Discovery. Discovery is the process of identifying devices that are connected to the network and retrieving information about those devices. Devices that can be discovered include laptops, desktops, servers, mobile devices, virtual devices, printers, network devices, wireless access points, routers, switches, and more. To discover devices on your network, create a Discovery Schedule. The Discovery Schedule specifies the protocols to use during the scan, the IP Address range to be scanned, and the frequency of the scan. You can scan for devices across a single subnet or multiple subnets.

Discovery uses the following protocols:

- Ping
- SNMP
- Socket
- NMAP
- Active Directory
- SSH/Telnet

Discovery Results show the availability and details of discovered devices. To manage discovered devices, install the K1000 Agent or enable Agentless management on the device.



Agentless device inventory

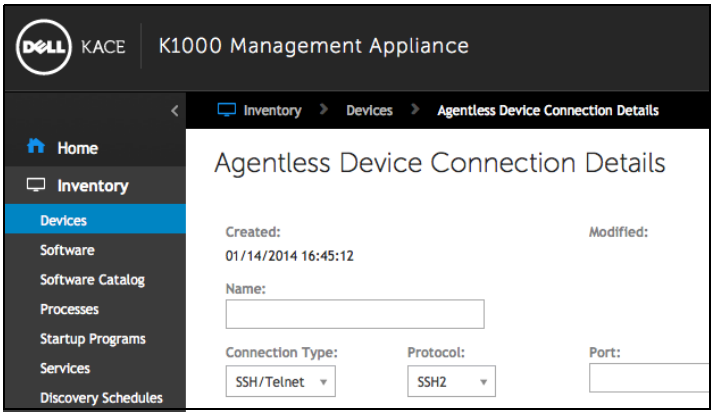
Version 6.0 brings Agentless device inventory to the K1000. Agentless device inventory enables you to manage devices in inventory without deploying and maintaining the K1000 Agent software on those devices. This is especially useful for:

- Agent-intolerant devices, such as printers, network devices, and storage devices
- Operating systems that are not supported by the K1000 Agent

Agentless management uses protocols such as SSH, Telnet, and SNMP to extract data from the remote device and report inventory in the K1000 Administrator Console. To enable Agentless management, you can use Discovery results or add device connection information manually.

Agentless management supports the following operating systems:

- AIX
- CentOS
- Debian
- Fedora
- FreeBSD
- HP-UX
- Oracle Enterprise Linux
- Red Hat
- Solaris
- SUSE
- Ubuntu



Features supported for Agentless device inventory

Device management features vary, depending on the method used to manage the device and the device's operating system. For Windows devices, installing the Agent provides a full range of features. When an Agent alternative is required, and for devices that cannot have the Agent installed, Agentless management is the

recommended option. For more information, see the *K1000 Administrator Guide,* http://www.kace.com/support/resources/documentation.

Agentless management features for Windows devices are limited to discovery only in the 6.0 release.

Agent-related enhancements

Agent-related enhancements include:

- **Additional operating system support**: The Agent can now be installed on, and used to manage, devices with the following operating systems:
  - Windows 8.1
  - Windows 2012 R2
  - Mac OS X 10.9
  - Ubuntu 13
- **Improved logging**: All Agent logs, such as AMP.log, klaunch.log, kdeploy.log, are now consolidated into a single log named Kagent.log. This consolidated log provides a correlated view of all Agent events. When the log reaches 4MB in size, it is moved to the backup area and a new log is started. The appliance saves the 5 most recent logs as backups.
- **User alert standardization**: Alerts that are displayed on Agent-managed Windows and Mac devices now use standardized dialogs and popups.
- **User alerts for all logged-in users**: When multiple users are logged in to an Agent 6.0-managed device, either on the device or through a remote desktop connection, alerts now appear on all user desktops. For Agent 5.5 and earlier, alerts were displayed only on the device (or on the first remote desktop) when multiple users were logged in.
- **Automatic grouping of deployed Agents**. Groups of deployed Agents can now be updated to a specified Agent version at specified times or on demand.
- **Add/Remove programs change**: K1000 Agent software no longer appears in the Add/Remove programs list on Windows devices. This reduces the possibility that end-users will remove the Agent from managed devices.

New icons for Agent-managed, Agentless, and manual devices

On Inventory pages, icons have been updated to communicate the status of devices in inventory:

: An Agent-managed device is connected to the appliance.

: An Agent-managed device is not connected to the appliance.

: Agentless management is enabled for the device.

: Agentless management is enabled for the device, but the device is not currently reachable.

: A manual device.

Application Control for Windows and Mac devices

You can now blacklist Software Catalog applications to prevent them from running on Agent-managed Windows and Mac devices. To enable Application Control, mark an application as Not Allowed, then apply the ApplicationControl label to Agent-managed devices. When the specified application is launched on a target device, the Agent terminates the application and displays an alert on the device explaining that the

application has been blacklisted. For more information, see the *K1000 Administrator Guide,* http://www.kace.com/support/resources/documentation.

Application Control is available only for Windows and Mac devices that have Agent version 6.0 software installed. Application Control is not available for Linux or Agentless devices.

K1000 GO enhancements

K1000 GO is the app that connects you to the K1000 from smart phones and tablets. Recent enhancements include:

- **Access for non-administrators**: Users who are not administrators can now log Service Desk tickets, view ticket status, and read Knowledge Base articles. The app detects user permission levels and adjusts the UI accordingly.
- **Service Desk enhancements**: You can now add photos to Service Desk tickets and edit additional ticket fields.
- **Bug fixes and UI improvements**: The app is continually being updated to fix issues and improve the user experience.

You can download K1000 GO from the Apple App Store for iOS devices, or from the Google Play Store for Android devices.

Terminology changes

Text in the UI has been updated to improve consistency and to use industry-standard terms. For example, the term *device* is now used to refer to machines, nodes, and computers in inventory. The following table shows terminology changes in this release.

Table-1: Terminology changes

5.5 terminology	6.0 terminology
Machine, node, computer, client	Device
Machine Action, Machine Label	Device Action, Device Label
Computer Asset	Device Asset
IP Scan	Discovery
Administrator Interface	Administrator Console
Command Line Interface	Command Line Console
User Portal	User Console
Allow List, Whitelist	Access Control List
Patch Listing	Patch Catalog
AppDeploy Live	ITNinja

Feature location changes

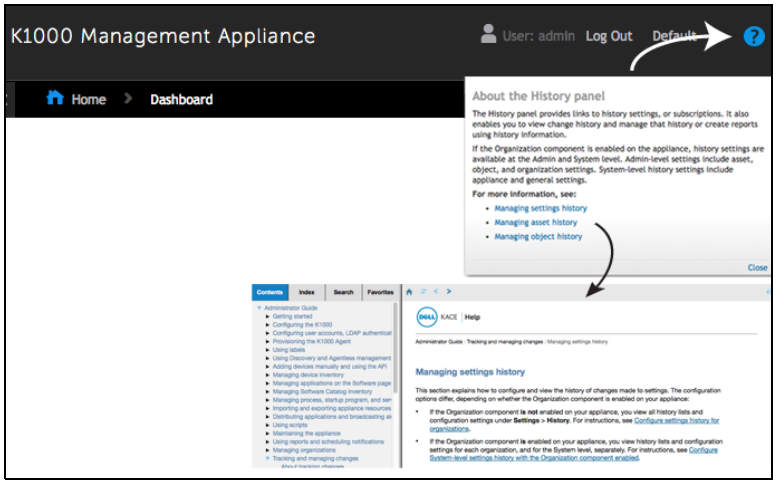
Some features have been moved to improve workflow. The following table shows feature location changes.

Table-2: Feature location changes

Feature	5.5 Location and name	6.0 Location and name
Dell Updates	Distribution > Dell Updates	Security > Dell Updates
Alerts for distribution to managed devices	Reporting > Alerts	Distribution > Alerts
Network scanning	Inventory > IP Scan	Inventory > Discovery Schedules Inventory > Discovery Results **Note**: Discovery Results can be used to help provision the Agent and enable Agentless management on devices.
Managing software for users to download	Service Desk > Software Library	Service Desk > User Console Library
Service Desk: Settings for All Queues on list pages	Service Desk > Configuration > Settings > Customize....	Service Desk > Configuration > Layout
Service Desk: Adding Ticket Rules	Service Desk > Configuration > Queues > Customize ...	Service Desk > Configuration > Rules
Information about the appliance or selected organization	Home > Summary Home > K1000 System Summary	Home > Dashboard Home > System Dashboard
Reports or alerts sent through email	Reporting > Email Alerts	Reporting > Notifications
K1000 Agent settings	Settings > K1000 Agent	Settings > Provisioning
System level features (available on appliances with the Organization component enabled)		
Control Panel settings	K1000 Settings > Control Panel	Settings > Control Panel
Users (System level)	K1000 Settings > Users	Settings > Administrators
Server Maintenance	K1000 Settings > Server Maintenance	Settings > Appliance Updates

Context-sensitive Help

Context-sensitive Help is now available for every page of the user interface. Previously, Help content appeared in the sidebar of some pages and was always displayed. This sidebar content has been removed, and the valuable screen real estate has been reclaimed for UI content.


K1000 Management Appliance
User: admin
Log Out
Default
Home
Dashboard
About the History panel
The History panel provides links to history settings, or subscriptions. It also enables you to view change history and manage that history or create reports using history information.
If the Organization component is enabled on the appliance, history settings are available at the Admin and System level. Admin-level settings include asset, object, and organization settings. System-level history settings include appliance and general settings.
For more information, see:
Managing settings history
Managing asset history
Managing object history
Close
Contents
Index
Search
Favorites
KACE | Help
Managing settings history

To open the context sensitive Help, click the **Help** button in the upper right of any UI page.

To access the main Help system, click the links in the context-sensitive Help topic. The main Help system includes the *Administrator Guide*, *Asset Management Guide*, *Patching and Security Guide*, and *Service Desk Administrator Guide* in both HTML and PDF formats. To access the PDFs, click the Home icon on the top bar of the main Help system:

End-of-life features

The following features are not supported in version 6.0 of the K1000 appliance and Agent:

- **Classic metering**: Classic Metering was the metering system available on the K1000 appliance prior to version 5.5. If you updated to version 5.5 from version 5.4 or lower, and you enabled metering prior to the update, you could continue to access Classic Metering in the K1000 5.5 release. However, Classic Metering is no longer available in version 6.0 and higher. The Software Catalog metering system, which provides more detailed information than Classic Metering, replaced Classic Metering in the 6.0 release.
- **Classic dashboards**: The classic dashboards have been replaced by new dashboards with customizable widgets in the 6.0 release.
- **Classic reports**: Classic reports are no longer available in the 6.0 release.
- **Hide from AppDeploy**. In version 5.5 and lower, you could select **Hide from AppDeploy** on software detail pages to prevent the K1000 from sharing anonymous information about the software with AppDeploy or ITNinja. This option is no longer available on the software detail pages. To control whether information is shared, configure data sharing options, which are available in the appliance's *General Settings*.
- **Operating systems**: The following operating systems are no longer supported by the K1000 Agent:
  - Mac OS X 10.5
  - Microsoft Windows 2000
  - RHEL 3
  - SUSE 12.1
- **Browsers**: The following browsers are no longer supported for accessing the Administrator Console and User Console:
  - Microsoft Internet Explorer 7.x
  - Mozilla Firefox 17.x - 19.x
  - Apple Safari 4.x

System requirements

For system requirements, go to http://www.kace.com/products/systems-management-appliance/tech-specs.

Updating the K1000 appliance (server)

Although Agent logs are routinely pruned on the K1000 appliance, this update **removes all log entries**. If this is an issue, contact Dell KACE Technical Support before attempting the update: http://www.kace.com/support/customer/tech-support.

Before you begin

Verify that your appliance meets the following requirements:

- **64-bit system**: If you have a physical K1000 appliance, it must be a 64-bit system. The 6.0 update cannot be installed on 32-bit appliances.
- **Current version**: The minimum version required for installing K1000 6.0 is **5.5 GA**. To check the version number of your appliance, log in to the Administrator Console, then click **About K1000** at the bottom left of the window. If your appliance is running an earlier version, you must update to the listed version before proceeding with the 6.0 installation.
- **Disk space**: You must have more than 15% free disk space available on the K1000 appliance. On physical appliances, this disk space must be on the appliance's main drive.

Additional recommendations:

- **Allow plenty of time**: If you have a large database, more than 150MB in size, the update process can take several hours.
- **Back up before you start**: Back up your database and files and save your backups to a location outside the K1000 server for future reference. For instructions on backing up your database and files, see the *K1000 Administrator Guide*, http://www.kace.com/support/resources/documentation. If your backup file (kbox_dbdata.gz) is more than 150MB in size, contact Dell KACE Technical Support for additional recommendations: http://www.kace.com/support/customer/tech-support.
- **Save patch notification messages**: If you have disabled patch progress notifications to managed devices, but you have notification message text that you want to keep, copy that text to a backup location. During the update, patch progress messages are deleted if patch progress notifications were disabled. See Verifying patch notification settings for patch schedules on page 12.
- **Enable SSH**: Enable SSH in the **Settings > Security Settings** section of the Administrator Console. This provides an easier path to recovery if necessary. When the update is successful, you can disable SSH as needed.
- **Know the version of deployed Agent software**: K1000 Agent software that is deployed on managed devices should be at version 5.5.30275 or higher. Older versions might not be able to communicate with version 6.0 of the K1000 server.

Updating the appliance

You can update the appliance using an advertised update or by manually uploading an update file.

Never manually reboot the appliance during an update.

Updating the appliance using an advertised update

You can update the appliance using an advertised update file.

Procedure

1. Back up your database and files. For instructions, see the *K1000 Administrator Guide*, http://www.kace.com/support/resources/documentation.
2. Log in to the Administrator Console and go to the appliance *Control Panel*:
   - If the Organization component is ***not*** enabled on the appliance: Log in to the K1000 adminui: `http://<K1000_hostname>/admin`, then click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the K1000 systemui: `http://<K1000_hostname>/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
3. Click the **Server Maintenance** tab.

   If the message, `Your K1000 is up to date` appears in the *Automatic K1000 Upgrade* section, no patches or updates are available.

   If the message, `Available Upgrade` appears, a patch or update is available.
4. If neither message appears, click **Edit Mode**.
5. In the *Automatic K1000 Upgrade* section, click **Check for Upgrade**.

   The *K1000 Server Logs* page appears. Results of the check appear in the log.
6. When an update is available, click **Upgrade Now**.

   The update is applied. The Administrator Console is unavailable until the update is complete. Progress appears in the browser window and in the Command Line Console.

   The appliance restarts when the update is complete.

Updating the appliance by manually uploading an update file

You can update the appliance by obtaining an update file and manually uploading it to the appliance.

Procedure

1. Back up your database and files. For instructions, see the *K1000 Administrator Guide*, http://www.kace.com/support/resources/documentation.
2. Using your customer login credentials, log in to the Dell KACE website at http://www.kace.com/support/customer/downloads.php, download the K1000 server **.kbin** file for the 6.0 GA (general availability) release, and save the file locally.
3. Go to the appliance *Control Panel*:
   - If the Organization component is ***not*** enabled on the appliance: Log in to the K1000 adminui: `http://<K1000_hostname>/admin`, click **Settings**.

- If the Organization component is enabled on the appliance: Log in to the K1000 systemui: `http://<K1000_hostname>/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

4. On the left navigation bar, click **Appliance Updates**.

   The *Appliance Updates* page appears.

5. In the *Manually Update* section:

   a. Click **Browse** or **Choose File**, and locate the update file.

   b. Click **Update**, then click **Yes** to confirm.

   The update begins. The Administrator Console is unavailable until the update is complete. Progress appears in the browser window and in the Command Line Console.

   The appliance restarts when the update is complete.

Post-update tasks

After the update, verify that the update was successful and verify settings as needed.

Verifying successful completion

Verify successful completion by reviewing the update log.

Procedure

1. Log in to the Administrator Console and go to the appliance *Control Panel*:
   - If the Organization component is ***not*** enabled on the appliance: Log in to the K1000 adminui: `http://<K1000_hostname>/admin`, click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the K1000 systemui: `http://<K1000_hostname>/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. Click **Logs**.

   The *Logs* page appears.
3. In the *Log* drop-down list, select **Server > Updates**.
4. Review the log for error messages and warnings.
5. Click **About K1000** in the bottom-left corner of the page to verify the current version.

Verifying security settings

To enhance security, database access over HTTP and FTP is disabled during the update. If you use these methods to access database files, change the security settings after the update as needed.

Procedure

1. Log in to the Administrator Console and go to the appliance *Control Panel*:
   - If the Organization component is ***not*** enabled on the appliance: Log in to the K1000 adminui: `http://<K1000_hostname>/admin`, click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the K1000 systemui: `http://<K1000_hostname>/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.

2. Click **Security Settings**.

   The *Security Settings* page appears.

3. In the top section of the page, change the following settings:

   - **Enable Secure backup files**: Clear this check box to enable users to access database backup files using HTTP without authentication.
   - **Enable Database Access**: Select this check box to enable users to access the database over port 3306.
   - **Enable Backup via FTP**: Select this check box to enable users to access database backup files using FTP.

   Changing these settings decreases the security of the database and is not recommended.

4. Click **Save**.

   The appliance restarts and the changes are applied.

Verifying patch notification settings for patch schedules

If *Show Patch Progress* is disabled on the *Patch Schedule Detail* page when the appliance is updated to version 6.0, the content of the patch progress message boxes is removed during the update. This prevents patch progress messages from being displayed on managed devices after the update. If you saved this message text before the update, you can replace it after the update when you want to enable patch progress notifications.

Text that appears in the message boxes in the *Notify* section is displayed as progress on managed devices during patching. To prevent the appliance from displaying progress messages, clear the message boxes.

Procedure

1. Log in to the K1000 adminui: `http://<K1000_hostname>/admin`. Or, if the fast switching option is enabled, select an organization in the drop-down list in the top-right corner of the page next to the login information.
2. Click **Security**.

   The *Patch Management* panel appears.

3. Click **Schedules**.

   The *Patch Schedules* page appears.

4. Do one of the following:

   - In the *Choose Action* menu, select **New**.
   - In the list of schedules, click the name of a schedule.

   The *Patch Schedule Detail* page appears.

5. In the *Notify* section, change settings as needed.

   Any text that appears in the *Initial Message*, *Progress Message*, and *Completion Message* text boxes is displayed on managed devices during patching. Version 6.0 of the K1000 server no longer has a separate check box to control whether progress messages are displayed.

Upgrading Agent software on managed devices

To take advantage of the many device-management features available in version 6.0 of the K1000 server, Agent software on managed devices must be upgraded. By default, the K1000 appliance checks with Dell KACE for Agent software updates at approximately 03:40 every day. In addition, the K1000 appliance checks with Dell KACE for Agent updates whenever the appliance is rebooted. When Agent updates are available, they are automatically downloaded to the K1000 appliance, provided that the appliance is connected to the Internet at that time.

Viewing Agent software updates

When an Agent update is available, an alert appears on the *Home* page of the K1000 Administrator Console. To view more information about the update, click the link in the Alert, or follow the instructions in this section.

Procedure

1. Log in to the K1000 Administrator Console and go to the appliance *Control Panel*:
   - If the Organization component is ***not*** enabled on the appliance: Log in to the K1000 adminui: `http://<K1000_hostname>/admin`, then click **Settings**.
   - If the Organization component is enabled on the appliance: Log in to the K1000 systemui: `http://<K1000_hostname>/system`, or select **System** in the drop-down list in the top-right corner of the page, then click **Settings**.
2. On the left navigation bar, click **Appliance Updates**.

   The *Appliance Updates* page appears. The current Agent bundle appears in the *Agent* section.
3. (Optional) To check for updates: In the *Agent* section, click **Check for Update**.

   The appliance checks for updates, and the results appear on the *Logs* page.

Loading Agent updates and configuring update settings

You load Agent updates to the K1000 server as described in this section. After you have loaded the Agent updates, they become available for installation on managed devices. If you have multiple organizations, you load Agent updates and configure update settings for each organization separately.

Agent-managed devices must have Agent version 5.5 GA or higher installed before they can be updated to Agent version 6.0. You cannot update managed devices from other versions directly to version 6.0.

The instructions in this section assume that the K1000 appliance has been updated to version 6.0. Instructions for previous versions are available in the *K1000 Administrator Guide*, http://www.kace.com/support/resources/documentation.

Procedure

1. Log in to the K1000 Administrator Console.
2. If applicable, select an organization in the drop-down list in the top-right corner of the page.
3. Click **Settings** > **Provisioning**.

   The *Provisioning* panel appears.

4. Click **Update Agents**.

   The *Update Agent Settings* page appears.

5. In the *Available Agent Bundle* section, click **Advertise**.

   The update is loaded and the new Agent software version number appears next to each operating system.

6. View or specify the Agent software update settings. For more information, see the *K1000 Administrator Guide*, http://www.kace.com/support/resources/documentation.

7. If you have multiple organizations, repeat the preceding steps for each organization.

Updating Agent software manually

Manually updating Agent software is useful if you need to update from older versions of the Agent software.

Agent-managed devices must have Agent version 5.5 GA or higher installed before they can be updated to Agent version 6.0. You cannot update managed devices from other versions directly to version 6.0.

To download the software, you must obtain customer login credentials by contacting Dell KACE Technical Support: http://www.kace.com/support/contact.php.

Procedure

1. Using your customer login credentials, log in to the Dell KACE website, http://www.kace.com/support/customer/downloads.php, download the Agent **.kbin** file for the 6.0 GA (general availability) release, and save the file locally.

The Agent software bundle that you upload to the K1000 server from this page should be an official Agent software release received from Dell KACE directly.

2. Log in to the K1000 Administrator Console.

3. If applicable, select an organization in the drop-down list in the top-right corner of the page.

4. Click **Settings** > **Provisioning**.

   The *Provisioning* panel appears.

5. Click **Update Agents**.

   The *Update Agent Settings* page appears.

6. In the *Manually Upload Agent Bundle* section, click **Browse** or **Choose File** and locate the update file that you downloaded in step 1.

7. Click **Upload**.

   The updated files appear in the *Loaded K1000 Agent Updates* section. The appliance installs the software update on managed devices according to the settings in the top section of the *Update Agent Settings* page.

8. If you have multiple organizations, repeat the preceding steps for each organization.

Stopping and starting the Agent

The procedures for stopping and starting the Agent service on devices running Mac OS X and Linux changed in Agent version 5.3. Use the procedures in this section to stop and start the 6.0 Agent on all versions of Mac OSX and Linux devices.

Stopping and starting the Agent on Mac OS X devices

Procedure

1. Open a terminal window on the Mac.
2. To stop the Agent, type the following:

   sudo /Library/Application\ Support/Dell/KACE/bin/AMPTools stop
3. To start the Agent, type the following:

   sudo /Library/Application\ Support/Dell/KACE/bin/AMPTools start

Stopping and starting the Agent on Linux devices

Procedure

1. Open a terminal window from **Applications** > **System Tools**.
2. To start the Agent, type the following:

   /opt/dell/kace/bin/AMPTools start
3. To stop the Agent, type the following:

   /opt/dell/kace/bin/AMPTools stop

Resolved issues

This section lists issues that have been resolved in this release.

Server-related resolved issues

This section lists server-related resolved issues.

Table-3: Server-related resolved issues

Issue Number	Title or Description
K1-10476	Custom inventory results are truncated at UTF characters.
K1-11604	System UI is not localized when non-English locale is selected.
K1-11978	The *Choose Action* menu in the Administrator Console does not work correctly when using the default document mode in Microsoft IE 10.
K1-12045	When you clone or duplicate a Service Desk ticket queue, the email address associated with the cloned queue is the same as the original queue. To resolve the issue, edit the cloned queue to change the email address.

Table-3: Server-related resolved issues (Continued)

Issue Number	Title or Description
K1-13281	The *Enable AppDeploy Live* check box no longer appears on the *General Settings* page, but it is referenced on some Administrator Console pages, including the *Managed Installations* page and the *Software Detail* page.
K1-13496	When a duplicate report name is detected during report creation, topic selections are reset.
K1-13777	The documentation incorrectly states that version-specific usage information is available for metered applications. Usage information is not available for each version of an application. Instead, the information is summarized for all versions of the application.
K1-13867	Service Desk ticket attachments cannot be downloaded using an Apple Safari browser on devices running Mac OS X.
K1-13891	When you add batch file steps to scripts using Microsoft IE 10 browser, quotation marks are mishandled.
K1-13917	Troubleshooting Tools Services checks fail when attempting to run MySQL database checks.
K1-14048	Email messages, with blank *To* field, are generated during scheduled LDAP imports.
K1-14050	Excessive database queries reduce Service Desk performance.
K1-14051	On x64 Windows devices, 32-bit application patches are not detected and deployed.
K1-14063	Search filters cause LDAP connection test failures.
K1-14071	When adding comments to Service Desk tickets, entering `TICK:<ticket_number>` no longer creates a hyperlink to the specified ticket.
K1-14076	During patch download, a MySQL `Access Denied` error message appears.
K1-14083	On the Service Desk Ticket Detail page, categories that are marked as Required appear on a separate line instead of next to the field name.
K1-14093 and K1-14057	On the *Inventory* > *Devices* page, Advanced search and Smart Label searches for *software publisher* or *software title* require excessive time to complete.
K1-14095	Global search requires excessive time to complete.
K1-14123	When LDAP user imports exceed the LDAP search limit, user names that include apostrophes, such as O'Brien, are excluded from import.
K1-14139	The License Compliance graph is not updated correctly on upgraded appliances.
K1-14246	When tables are used in Knowledge Base articles, the Markdown function results in excessive whitespace or blank lines.
K1-14329	Appliance backup does not include MySQL database and tables.
K1-14632	Email notifications are sent incorrectly after cron jobs run.
K1-14736	Assigning a label group to a Replication Share converts the label group to a standard device label and breaks the label group association.
K1-14777	When the database is restored from backup, resources exported to the local K1000 are restored to the database. However, the `/kbox/kboxwww/resources` directory is not backed up as part of the nightly backup routine. This results in a list of resources that fail to import due to missing resource packages.

Table-3: Server-related resolved issues (Continued)

Issue Number	Title or Description
K1-14810	Reports that break on headings are truncated when sections contain a single sub-item.
K1-15001	In the Service Desk Customer Satisfaction Survey, comments longer than a single line are not wrapped to the next line. Instead, they scroll off the page.
K1-15029	When assets are imported from CSV files to fields with *Allow Multiple* enabled, *Text* and *Note* fields are duplicated.
K1-15075	The *Provisioned Configuration* list displays incorrectly and hangs on systems with 90,000 items in the list. **Note**: The *Provisioned Configuration* list has been renamed *Provisioning Schedules*.
K1-15097 and K1-14100	When the *Owners Only* status of Service Desk tickets is changed, timestamps are removed from comments.
K1-15345	To sort the *Inventory* > *Computers* page by the *Last Sync* column, you have to click the column heading twice. **Note**: The *Computers* page has been renamed *Devices*, and the *Last Sync* column has been renamed *Last Inventory*.
K1-15388	In the Service Desk Software Library, the word *Install* is displayed incorrectly in the *Name* column of non-Windows software.
K1-15510	Unused packages for disabled patches are not cleaned up when patches are deleted.
K1-15535	Custom logo images are broken in HTML reports delivered through email.
K1-15634	When Replication Shares are used for patching, the SMB path and credentials are provided as clear text for each of the handshake files.
K1-15701	On the *Patch Catalog* page, the *View By* list shows incorrect results for the *All Patches* view.
K1-15751	Wizard-created Inventory reports that use Asset fields do not run correctly.
K1-15753	When patches with multiple signatures are deployed, the `Fail 84` error message appears.
K1-15966	When using Google Chrome browser, scroll bars do not work correctly with Smart Labels.

Agent-related resolved issues

This section lists Agent-related resolved issues.

Table-4: Agent-related resolved issues

Issue Number	Title or Description
KA-73	Agent logs should clearly describe errors that occur when the K1000 license limit has been reached or exceeded.
KA-131	RHEL 5 SSL certificate location affects authentication.
KA-140	KInventory.exe crashes prevent managed devices from checking in to the K1000.

Table-4: Agent-related resolved issues (Continued)

Issue Number	Title or Description
KA-151	Using GPO (Group Policy Object) to install the K1000 Agent results in duplicate entries in the *Add/Remove* programs list. The K1000 6.0 version of the Agent no longer appears in the Add/Remove programs list.
KA-177	On Agent-managed Mac devices, the **kdeploy** log does not display commands used to deploy packages.
KA-199	In Custom Inventory rules, *ShellCommandTextReturn* does not return results for *net localgroup administrators*.
KA-204	When the company name is changed to use Japanese or other unicode characters in the appliance *General Settings*, deployed Agents on managed devices fail to report inventory.
KA-208	For deploy-only patching schedules, alert messages are not displayed correctly after managed devices reboot.
KA-230	Managed devices running Mac OS 10.9 cannot update to Agent version 5.5.
KA-258	Managed Installations with batch scripts that have CMD filename extensions do not run on managed devices.
KA-294	Agent alert messages that have more then five lines cannot be viewed correctly on managed devices because the alert window does not have a scroll bar.
KA-306	Agent logs are truncated for large patching schedules.
KA-311	When metering is enabled for an application, and the application is uninstalled on a managed device, the folder that contained the application is locked until the device restarts.
KA-337	`System Error 183` appears when patch schedules run on managed devices that are running Remote Desktop (RDP) sessions. **Note**: On Windows 2003 and Windows XP devices, patches continue to deploy successfully when RDP sessions are connected, and alerts are not displayed on RDP sessions. Alerts are displayed only on console sessions.
KA-376	When `runkbot 2 0` runs on an Agent-managed Linux device, the following message appears: `sh: KACE_SPLASH_TEXT: command not found`.
KA-409	In Managed Installations that contain ZIP files, the Agent changes filenames that contain special characters, such as accent marks, when the files are unzipped.
KA-410	The DWORD type registry value is incorrectly retrieved as 0, and verification fails if DWORD is any other value.
KA-416	Win32_DesktopMonitor information from WMI (Windows Management Instrumentation) is not translated from **kinventory.db** to **kinventory.xml**.
KA-433	When files larger than 2GB are replicated, and bandwidth restriction is enabled, the files continue grow in size until they are deleted.
KA-479	If the `NOHOOKS=1` option is used during Agent installation, Userinit settings are incorrect after Agent updates.
KA-493	Account credentials are displayed in clear text during Replication Share access.
Agent-1870	Managed Installations and File Synchronizations fail to download from Replication Shares when the Replication Shares are located on devices running a Mac OS.

Table-4: Agent-related resolved issues (Continued)

Issue Number	Title or Description
Agent-3955	On managed devices running Red Hat Enterprise Linux 7, timezone information for the K1000 Agent is not available.

Known issues

This section lists known issues in this release.

Server-related known issues

This section lists server-related known issues.

Table-5: Server-related known issues

Issue Number	Title or Description
K1-9245	When two different managed devices are assigned the same IP address, the devices are not identified as separate devices, and inventory information is recorded incorrectly.
K1-9523	Incorrect data is displayed when you create a report using the wizard with the *Computer Disk* report topic.
K1-9829	Scheduled report search does not search translated built-in report names.
K1-10411	Tickets sent using the “email ticket” feature are missing the server name in attachment URLs.
K1-10626	The appliance does not validate manually imported XML inventory data that is uploaded using WSAPI. As a result, invalid inventory information might be displayed for manual device records if the XML is invalid.
K1-10769	Localized search is not supported. Incorrect data is displayed when you create a report using the wizard with the *Computer Disk* report topic, and scheduled report search does not search translated built-in report names.
K1-12082	When you archive Service Desk tickets, attachments are not moved; they remain in the attachments area on the server.
K1-12374	Attachments in Service Desk tickets can be accessed only from links within the tickets. If you try to access attachments by entering their URLs outside of Service Desk tickets, the message, `Permission denied` appears.
K1-12375	The *Choose Action* and *View By* drop-down lists in the Administrator Console are not displayed correctly when viewed in Microsoft IE 10, with the locale set to a non-English language, and Enhanced Security Configuration enabled.
K1-12836	In the new metering system, operating system software cannot be metered. However, when you attempt to enable metering for operating system software on the *Software Catalog* page, the Administrator Console provides no feedback to indicate that the software cannot be metered.
K1-13190	In the Reporting section, the *Select All* check box for *Other* is displayed as unchecked, even if the *Number of Records Analyzed* field is selected.

Table-5: Server-related known issues (Continued)

Issue Number	Title or Description
K1-13290	On the *Script Detail* page, custom schedules are saved without validation. As a result, if you enter and save an invalid custom schedule, the schedule is saved but it does not run correctly.
K1-13277	The K1000 does not add devices for Wake-on-LAN if the devices do not have hostnames.
K1-13455	When you enable POP3 on the Service Desk queue configuration page, email messages are not delivered appropriately until the K1000 appliance is restarted manually.
K1-13457	Locally Cataloged mobile applications cannot be added to a license asset.
K1-15114	In Agentless device inventory results, *Chassis Type* is set to *Unknown* for SNMP-based devices.
K1-15217	When you use Advanced Search on the *Patch Catalog* page to search for Windows 8.1 patches, Windows 8 patches are included in the search results.
K1-15472	The Service Desk ticket email system has an 8MB size limit on attachments. Attachments that exceed 8MB in size are rejected, and no error message is displayed to the sender.
K1-15494	Windows Store applications can be launched on Windows 8 devices even when the applications are marked as Not Allowed.
K1-15940	Patch detection jobs time-out after 60 minutes. Therefore, if the patch job goes over the time limit, the status of the job is reported as *Error*. This 60-minute time-out limit is not documented in the *K1000 Administrator Guide*.
K1-15988	SSL is automatically enabled for AMP connections if SSL is enabled in the appliance security settings. The controls are no longer separate. When you select the check box labeled, **Enable SSL** on the *Agent Settings* page, the following error message appears: `SSL settings can be enabled or disabled on the Security Settings page`.
K1-16120	When you connect to the appliance using web-based VPN software, some pages might not display data correctly. For example, list pages might be empty. This is because some VPN software, such as Cisco SSL VPN, modifies the contents of web pages as they pass from the K1000 to the browser. The VPN software does this to modify links to point to the VPN and to insert a VPN toolbar on the screen to control the connection. However, these modifications can interfere with the Javascript used by the K1000 to display the Dashboard and list pages. To avoid the issue, upgrade your web-based VPN software or use a client-based VPN when accessing the K1000.
K1-16362	After uninstalling the Agent from a managed device using a provisioning schedule, the Provisioning Results page displays errors when the locale is set to non-English languages, including French, Japanese, Chinese, and Portuguese.
K1-16433 **K1-16434**	During the update to 6.0, HTTP and FTP access to database backup files is disabled to enhance security. For more information, see Verifying security settings on page 11.

Table-5: Server-related known issues (Continued)

Issue Number	Title or Description
K1SD-2249	If the *Title* field is marked as hidden in a Service Desk ticket queue, errors are reported when you edit Process tickets in that queue. To prevent errors, temporarily mark the hidden *Title* field as visible, modify the Process ticket, then mark the *Title* field as hidden again.
N/A	Service Desk ticket rules that refer to HD_QUEUE custom fields fail because HD_QUEUE is moved to HD_FIELD during the K1000 server update to version 6.0. To resolve the issue, rewrite ticket rules to use HD_FIELD.
N/A	K1000 version 5.5 had a *Show Patch Progress* check box on the *Patch Schedule Detail* page. This check box controlled whether patch progress messages appeared on managed devices during patching. In version 6.0, the *Show Patch Progress* check box has been removed. To prevent patch progress messages from being displayed on managed devices, delete the contents of the message boxes (*Initial Message*, *Progress Message*, and *Completion Message*) in the *Notify* section of the *Patch Schedule Detail* page (**Security > Schedules > Schedule Detail**). If *Show Patch Progress* is disabled when the appliance is updated to version 6.0, the content of the message boxes is removed. This prevents patch progress messages from being displayed on managed devices after the update. For more information, see Verifying patch notification settings for patch schedules on page 12.

Agent-related known issues

This section lists Agent-related known issues.

About Agent security

Two amp.conf SSL settings are implemented on the K1000 Agent: **sslrequired** and **`verifyssl`**. Both settings are disabled by default, and they have to be set manually using AMPTools.

Enabling **sslrequired** in amp.conf (using a value of either `yes` or `true`), forces the Agent to connect to the appliance using HTTPS over port 443 for both AMP and web connections. As a result, if the appliance is not configured to use port 443, the Agent disconnects. Uploads and downloads are also performed through HTTPS when **sslrequired** is enabled because the regular fall back to HTTP is disabled.

Enabling **verifyssl** provides a higher level of security than **sslrequired** alone. When **verifyssl** is enabled in amp.conf (using a value of either `yes` or `true`), the Agent validates the K1000 server certificate against the list of known certificate authorities listed in **cacert.pem** in the data directory. The certificate bundle is exported from Mozilla and shipped with the Agent installation by default. Turning on **verifyssl** implies **sslrequired**, so the Agent cannot connect if port 443 is not configured. Verifying the server certificate means the certificate must be up to date, the server name must match, and the certificate must be traced back to a trusted authority listed in the certificate bundle.

In version 6.0, self-signed certificates are not supported because they are not listed as trusted authorities in the certificate pem file. As a result, Dell KACE recommends that you enable **verifyssl** only if the server has a publicly signed valid certificate. Otherwise the Agent cannot connect to the K1000 appliance.

Use the following commands to enable SSL in AMPTools:

```
AMPTools set sslrequired=true
AMPTools set verifyssl=true
```

For Mac and Linux devices, AMPTools is located under the Agent bin folder. For Windows devices AMPTools is located in `%ProgramFiles%\Dell\KACE`

There is a condition under which amp.conf can be blanked out or emptied. If that happens, the Agent's settings are lost, and it falls back to connect to `KBOX`. If an attacker poses as `KBOX` on the network, the Agent becomes open to attack even if it was originally configure with **verifyssl**. Dell KACE is investigating the cause of this issue.

Table-6: Agent-related known issues

Issue Number	Title or Description

Agent-1712	When the K1000 Agent is installed or uninstalled manually, the Agent's version number is not displayed on the wizard installation and uninstallation screens. To view the current installed version, do one of the following:
	• **Windows x64**: Open a command prompt and run the following command:
	`wmic datafile where name='c:\\program files (x86)\\dell\\kace\\AMPTools.exe' get version`
	• **Windows x86**: Open a command prompt and run the following command:
	`wmic datafile where name='c:\\program files\\dell\\kace\\AMPTools.exe' get version`
	• **Mac OS**: Using a terminal, run the following command:
	`sudo /Library/Application Support/Dell/KACE/bin/AMPTools get version`
	• **Linux**: Using a terminal, run the following command:
	`sudo /opt/dell/kace/bin/AMPTools get version`

Agent-1891	Managed Installations that are scheduled to run at startup fail on devices running Windows 2003 (64-bit) and Windows XP (64-bit) if Microsoft hotfix KB942589 (http://support.microsoft.com/kb/942589) is not installed prior to K1000 Agent installation. To resolve the issue, uninstall the K1000 Agent, install the hotfix, then reinstall the K1000 Agent.
Agent-2230	When replicated inventory is deleted manually, the K1000 Agent still reports files as present in inventory updates.
Agent-3316	Installing the K1000 Agent using Group Policy fails when the target operating system language (locale ID) is not defined by the installer.To resolve the issue, change the locale ID of the installer to the appropriate locale. To obtain a script that changes the locale ID, go to the Dell KACE knowledge base: http://www.kace.com/support/resources/kb/solutiondetail?sol=SOL111244.
Agent-3978	The catalog-based software inventory collection process has a dependency on WMI (WIndows Management Instrumentation). As a result, if the WMI service is not running, or if the WMI database is corrupted, the process fails to collect software inventory information.
KA-475	Online KScript alert messages appear on all logged in sessions regardless of the *Run as User* setting.

Table-6: Agent-related known issues (Continued)

Issue Number	Title or Description
KA-704	On Mac and Linux devices, Agent updates to version 6.0 fail when using Replication Shares with the *Failover To Appliance* option selected. This option is not supported with Replication. When using Replication Shares, disable *Failover To Appliance* before you update Agents to 6.0 on Mac and Linux devices.
KA-722	On Linux devices, the Agent does not process the bootstrap request when it receives a request to generate a new KUID. The bootstrap request is processed only after the Agent is restarted.

Agentless- and Discovery-related known issues

This section lists Agentless- and Discovery-related known issues.

Table-7: Agentless- and Discovery-related known issues

Issue Number	Title or Description
IME-288	For IP Scan results (Discovery Results) generated prior to version 6.0 of the K1000, the Created and Seconds fields appear blank in the K1000 Administrator Console. To populate the fields, open, save, and run the scan.
IME-294	Agentless inventory collection is disabled when inventory tasks are deleted from the Agent Tasks list at the system level: **Settings** > **Support** > **Troubleshooting Tools - View agent command queue**. To collect inventory information for a device after the inventory task has been disabled, go to the *Device Detail* page: **Inventory** > **Devices** > <*Device name*>.
IME-308 and IME-368	Advanced search options do not include Agentless device connection protocols, such as SSH and SNMP, or device connection time. For Agentless devices, the *Last Sync Time* field indicates the last time the K1000 connected to the device and collected inventory.
IME-336	SNMP Discovery does not capture device *Name* and *Location* information unless full walk is selected.
IME-429	When using SSH or Telnet as the Discovery method, devices whose SSH/Telnet ports are not set to the default port (22/23) will render unsuccessful for that test. Using an alternative method, such as Ping or Socket, might offer success and reachable status.

Documentation-related known issues

This section lists documentation-related known issues.

Table-8: Documentation-related known issues

Issue Number	Title or Description
N/A	In the Agent settings section of the *K1000 Administrator Guide*, the description of the *Disable duplicate device detection* option is incorrect. When the option is selected, duplicate device detection is disabled, and Agents do not receive requests to generate new IDs for devices and reconnect. Do not select this option unless you have discussed the ramifications with Dell KACE Technical Support.

K1-16387
K1-16429
	Localized versions of the documentation (online Help and PDFs) do not include the following updates:
	• The following website must be accessible to the appliance: https://servicecdn.kace.com.
	• The following information about ports that must be accessible to the appliance has changed:
	  • Ports 20 and 21 (**inbound** to the appliance) are used to access backup files on the appliance through FTP from outside the firewall. These ports are optional and not recommended.
	  • Port 22 (**outbound** from the appliance) is used to create an SSH tunnel to kace.com.
	  • Port 23 is not used.
	  • Ports 8080 and 8443 are no longer required for reporting.
	• On the *Patch Schedule Detail* page, the **Run on next connection if offline** is available. This option runs the action the next time the managed device connects to the appliance, if the device is currently offline. If the option is not selected, and the device is offline, the action does not run again until the next scheduled time.
	• In the *Managed Installations* section, the following information was clarified: The appliance uses a Replication Share before it uses the KACE Alt Location.
	• In the *Configure Agent Settings* procedure, *Enable SSL* is a read-only field. Agent SSL settings are controlled by the appliance security settings.

Global support

For information regarding the latest available firmware, release note revisions, or additional assistance, see the Dell KACE Support website: http://www.kace.com/support.

Copyright notice

© 2004-2014 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden. Dell and the DELL logo are trademarks of Dell Inc. Other trademarks and trade names may

be used in this document to refer to either the entities claiming the marks or the names of their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

This product is protected by U.S. Patent # 7,814,190; 7,818,427; 7,890,615; 8,103,751; 8,301,737; and 8,381,231. For more information, go to http://software.dell.com/legal/patents.aspx.

May 2014 Rev. A00